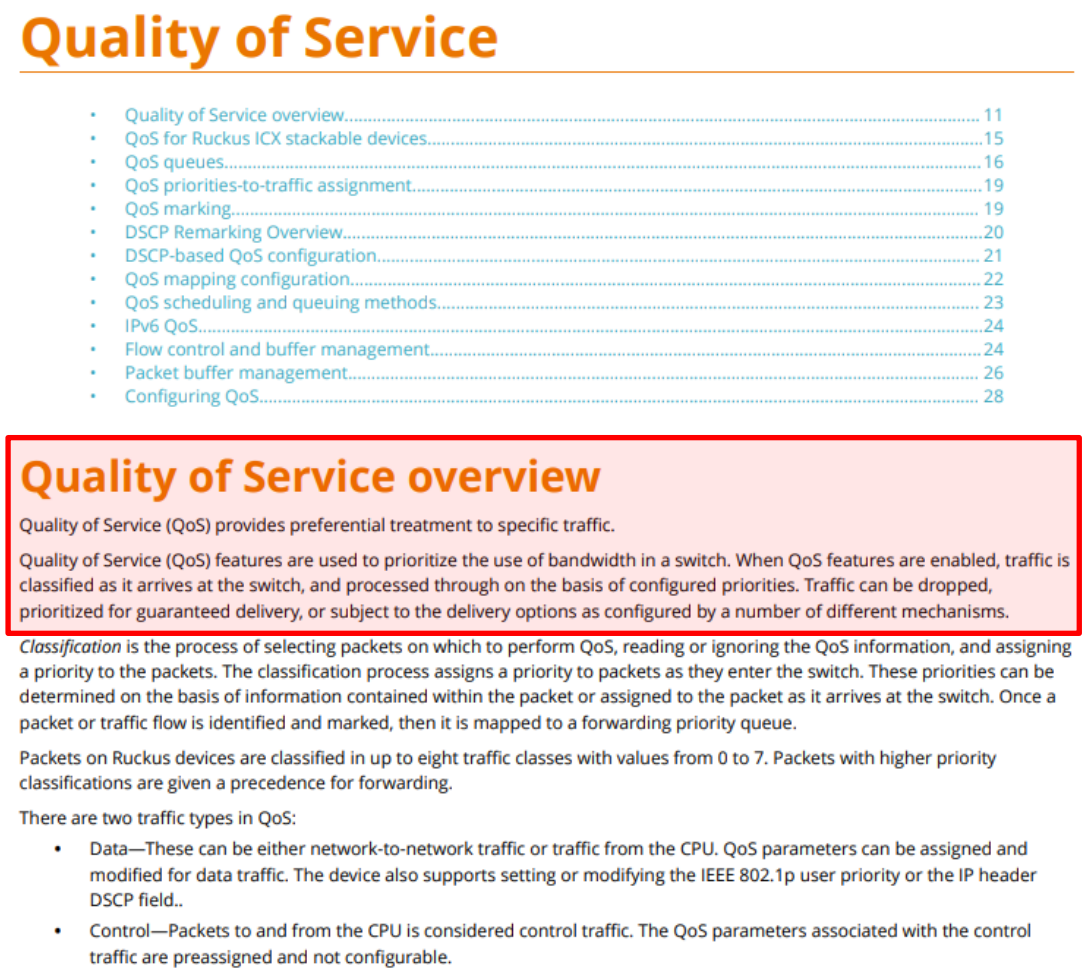
EXHIBIT E

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	**The Ruckus Devices comprise wireless access points and routers that allow for encrypted creation of Quality of Service ("QoS") steams. The Ruckus Devices include, but are not limited to the R730 Nighthawk router. The Ruckus Devices perform a method for transferring data with a verified QoS in a communication network. The Ruckus Devices support Quality of Service ("QoS") which prioritizes packets for certain types of traffic on the wireless network it deploys.** 

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	**NEW RUCKUS R730 IS THE FIRST IOT- AND LTE-READY 802.11AX ACCESS POINT FOR STADIUMS, PUBLIC VENUES, TRAIN STATIONS AND SCHOOLS** Company also launches Ultra-High Density Technology Suite that enhances network performance and WPA3 security compliance to protect end-users from common attacks **SUNNYVALE, Ca., July 17, 2018** – Ruckus Networks, an ARRIS company, today announced the Ruckus R730, the industry's first IoT- and LTE-ready, 802.11ax wireless access point (AP). The high-capacity, 12 spatial-stream R730 works in concert with the new Ruckus Ultra-High Density Technology Suite to smoothly deliver high-resolution, latency-sensitive video in ultra-high density user environments such as stadiums, train stations and schools. In addition, the R730 complies with both the new WPA3™ security protocol and Wi-Fi™ Enhanced Open for more secure connections on public networks. Worldwide data and video traffic is growing at double-digit rates, driven by an increase in connected devices. ABI Research predicts that Wi-Fi device shipments will grow to nearly 35 billion by 2022. Data and video traffic also will surge due to increased per-device data consumption driven by applications like 4K video streaming, virtual and augmented reality and live-stream gaming. "Ruckus customers and partners demand more when it comes to their networks," said Ian Whiting, president of Ruckus Networks. "We have a long history of delivering products and technologies that go beyond the current state-of-the-art to meet the world's most demanding network requirements while driving down the cost-per-connection. Ruckus R730 and Ruckus Ultra-High Density Technology Suite are the latest examples." The congestion of people, devices and bandwidth-hungry apps makes for challenges that current wireless tech cannot handle. Adding to the complexity of this environment are diversifying device categories and apps, such as instant messaging, IoT control messages and voice-over-Wi-Fi. "Real-world use cases are bumping up against the limits of existing Wi-Fi standards, and the need for 802.11ax to address a wide variety of heterogeneous, high-density scenarios is clear," said Chris DePuy, founder and technology analyst at 650 Group. "Ruckus has already differentiated itself in the realm of network consolidation. With this launch, Ruckus is reinforcing that by setting the stage for converged Wi-Fi, IoT and LTE deployments." **802.11ax: More connections and bandwidth, higher QoS** The new 802.11ax standard was designed for high-density connectivity, with the ability to support up to a four-fold capacity increase over its 802.11ac Wave 2 predecessor. With 802.11ax, multiple APs used in dense device environments are collectively able to deliver required quality-of-service (QoS) to more clients with more diverse usage profiles due to the use of orthogonal frequency-division multiple access (OFDMA) and multi-user multiple-in multiple-out (MU-MIMO) technologies. **Source: https://www.ruckuswireless.com/press/releases/20180717-new-ruckus-r730-first-iot-and-lte-ready-80211ax-access-point-stadiums-public**

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	

Quality of Service

Quality of Service overview

Quality of Service (QoS) provides preferential treatment to specific traffic.

Quality of Service (QoS) features are used to prioritize the use of bandwidth in a switch. When QoS features are enabled, traffic is classified as it arrives at the switch, and processed through on the basis of configured priorities. Traffic can be dropped, prioritized for guaranteed delivery, or subject to the delivery options as configured by a number of different mechanisms.

Classification is the process of selecting packets on which to perform QoS, reading or ignoring the QoS information, and assigning a priority to the packets. The classification process assigns a priority to packets as they enter the switch. These priorities can be determined on the basis of information contained within the packet or assigned to the packet as it arrives at the switch. Once a packet or traffic flow is identified and marked, then it is mapped to a forwarding priority queue.

Packets on Ruckus devices are classified in up to eight traffic classes with values from 0 to 7. Packets with higher priority classifications are given a precedence for forwarding.

There are two traffic types in QoS:

- Data—These can be either network-to-network traffic or traffic from the CPU. QoS parameters can be assigned and modified for data traffic. The device also supports setting or modifying the IEEE 802.1p user priority or the IP header DSCP field..
- Control—Packets to and from the CPU is considered control traffic. The QoS parameters associated with the control traffic are preassigned and not configurable.

Source: Ruckus FastIron QoS and Traffic Management Configuration Guide, 08.0.90, p. 11

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	

A Brief Introduction to IEEE 802.11e

In IEEE 802.11e, two types of QoS are identified – prioritized QoS and parameterized QoS. Prioritized QoS is a weak requirement that enforces relative priority between traffic classes. Parameterized QoS, on the other hand, is a strict requirement expressed quantitatively in terms of the QoS parameters.

A new access mechanism (called as HCF – Hybrid Coordination Function) has been defined with EDCA for contention based and HCCA for contention free access methods. Please recall that DCF is contention based while PCF is contention free access methods in 802.11

A few additional mechanisms have been added to improve channel utilization and efficiency. These are "Block Acknowledgement", "Direct Link Setup", "Automatic Power Save Delivery" among others.

The 802.11 header has been modified to add a new field to classify the type of traffic. The TID (traffic ID) is used to select a UP (user priority) for prioritized QoS or a TSPEC (traffic specification) for parameterized QoS. TID values between 0 – 7 are considered user priorities and these are identical to the IEEE 802.1D priority tags. TID values between 8 – 16 refer to TSPECs.

A TSPEC between an AP and an STA is negotiated by means of new management commands – ADDTS Request, ADDTS Response and DELTS. After a TSPEC is successfully negotiated, an STA can get a TXOP by one of two ways:

- Using EDCA, an STA can contend for the medium, and if it acquires the medium can use the medium for TXOP time limit. The STA must observe the TXOP time limit as specified in an IE in beacons.
- During CP/CFP, an AP can grant an STA a TXOP using the QoS CF-Poll (called as "polled TXOP" in contrast to "EDCA TXOP"). The TXOP limit is specified in the CF-Poll frame. While the spec allows an AP to grant a "polled TXOP" to an STA during either CFP or CP, it is recommended that it not be issued during CFP, but only during CP for reasons of simplicity in implementation.

Wireless Media Extensions (WME)

Wireless Media Extensions (WME), also referred to as WiFi Multimedia (WMM), is an industry driven initiative to ensure that a basic subset of IEEE 802.11e QoS mechanisms are interoperable. As such, WME supports only EDCA but not HCCA. Without HCCA, parametererized QoS can not be supported. As mentioned earlier, prioritized QoS identifies four traffic classes (or Access Categories) with differing priorities. The 8 user priorities of 802.1D map to these 4 ACs. Also, the Atheros code maps TOS fields in IP headers to these 4 ACs.

AC Number	Name	Description
0	BE	Best effort
1	BK	Background
2	VI	Video
3	VO	Voice

Source: http://wifi-insider.com/wlan/wmm.htm

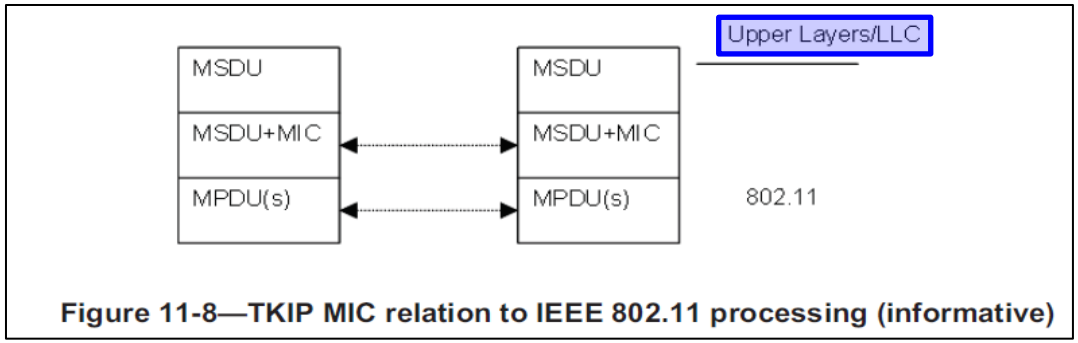
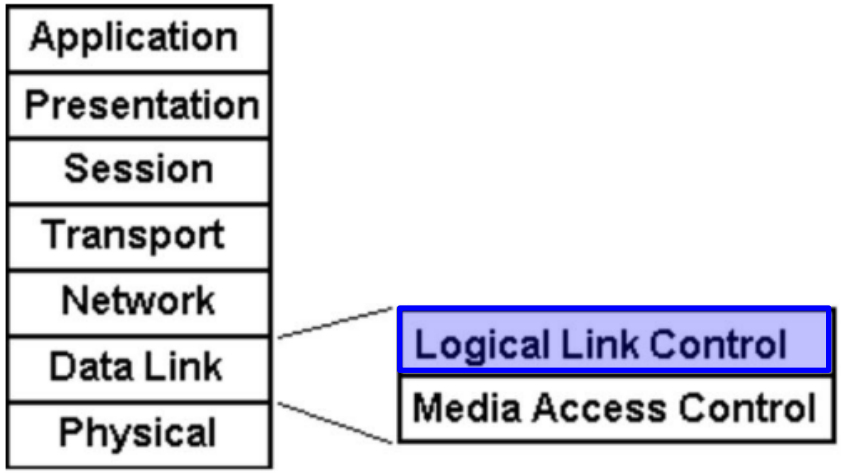
Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	**The Ruckus Devices provide a communication network, the WiFi network.** The R730 when paired with the Ruckus Ultra-High density Technology Suite found only in the Ruckus Wi-Fi portfolio, dramatically improves network performance through a combination of patented wireless innovations and learning algorithms that includes: • **Airtime Decongestion:** Increases average network throughput in heavily congested environments • **Transient Client management:** Reduces interference traffic from unconnected Wi-Fi devices • **BeamFlex+ Antennas:** Extended coverage and optimized throughput with patented multi-directional antennas and radio patterns Whether you're deploying ten or ten thousand APs, the R730 is also easy to manage through Ruckus' appliance and virtual management options. **Source: Ruckus R730 Data Sheet, p. 1** **When QoS is enabled, the Ruckus Devices transfer data with a verified QoS. The MSDU constitutes data with a verified QoS.** **4.5.2.3 QoS traffic scheduling** QoS traffic scheduling provides intra-BSS QoS frame transfers under the HCF, using either contention-based or controlled channel access. At each TXOP, a traffic scheduling entity at the STA selects a frame for transmission, from the set of frames at the heads of a plurality of traffic queues, based on requested UP and/or parameter values in the traffic specification (TSPEC) for the requested MSDU. Additional information is available in 9.19. **Source: 802.11 § 4.5.2.3**

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	**8.2.4.5 QoS Control field** **8.2.4.5.1 QoS Control field structure** The QoS Control field is a 16-bit field that identifies the TC or TS to which the frame belongs as well as various other QoS-related, A-MSDU related, and mesh-related information about the frame that varies by frame type, subtype, and type of transmitting STA. The QoS Control field is present in all data frames in which the QoS subfield of the Subtype field is equal to 1 (see 8.2.4.1.3). Each QoS Control field comprises five or eight subfields, as defined for the particular sender (HC or non-AP STA) and frame type and subtype. The usage of these subfields and the various possible layouts of the QoS Control field are described 8.2.4.5.2 to 8.2.4.5.12 and illustrated in Table 8-4. See 9.12.1 for constraints on the contents of the QoS Control field when present in an A-MPDU. **Source: 802.11 § 8.2.4.5** **4.5.6 Traffic differentiation and QoS support** IEEE Std 802.11 uses a shared medium and provides differentiated control of access to the medium to handle data transfers with QoS requirements. The QoS facility (per MSDU traffic category and TSPEC negotiation) allows an IEEE 802.11 LAN to become part of a larger network providing end-to-end QoS delivery or to function as an independent network providing transport on a per-link basis with specified QoS commitments. The specifications regarding the integration and operability of the QoS facility in IEEE 802.11 specification with any other end-to-end QoS delivery mechanism like Resource Reservation Protocol (RSVP) are beyond the scope of this standard. **Source: 802.11 § 4.5.6**

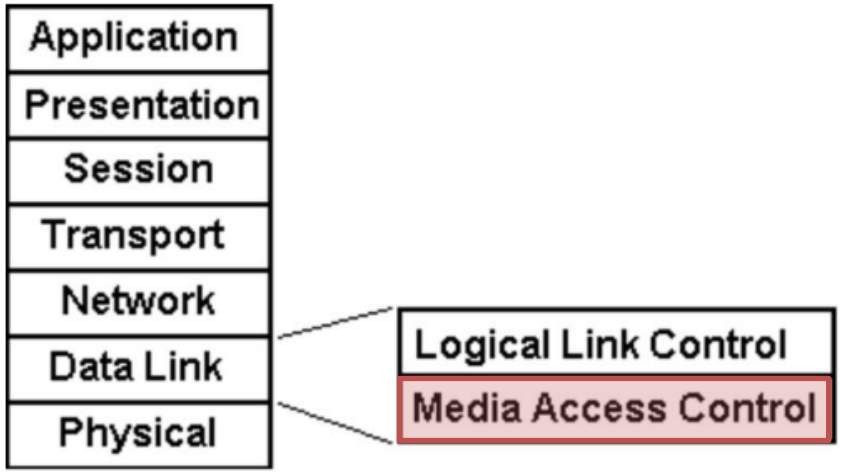
Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	Table 8-4—QoS Control field

Applicable frame (sub) types	Bits 0–3	Bit 4	Bits 5-6	Bit 7	Bits 8	Bit 9	Bit 10	Bits 11-15
QoS CF-Poll and QoS CF-Ack+CF-Poll frames sent by HC	TID	EOSP	Ack Policy	Reserved	TXOP Limit			
QoS Data+CF-Poll and QoS Data+CF-Ack+CF-Poll frames sent by HC	TID	EOSP	Ack Policy	A-MSDU Present	TXOP Limit			
QoS Data and QoS Data+CF-Ack frames sent by HC	TID	EOSP	Ack Policy	A-MSDU Present	AP PS Buffer State			
QoS Null frames sent by HC	TID	EOSP	Ack Policy	Reserved	AP PS Buffer State			
QoS Data and QoS Data+CF-Ack frames sent by non-AP STAs that are not a TPU buffer STA or a TPU sleep STA in a nonmesh BSS	TID	0	Ack Policy	A-MSDU Present	TXOP Duration Requested			
	TID	1	Ack Policy	A-MSDU Present	Queue Size			
QoS Null frames sent by non-AP STAs that are not a TPU buffer STA or a TPU sleep STA in a nonmesh BSS	TID	0	Ack Policy	Reserved	TXOP Duration Requested			
	TID	1	Ack Policy	Reserved	Queue Size			
QoS Data and QoS Data+CF-Ack frames sent by TPU buffer STAs in a nonmesh BSS	TID	EOSP	Ack Policy	A-MSDU Present	Reserved			
QoS Null frames sent by TPU buffer STAs in a nonmesh BSS	TID	EOSP	Ack Policy	Reserved	Reserved			
QoS Data and QoS Data+CF-Ack frames sent by TPU sleep STAs in a nonmesh BSS	TID	Reserved	Ack Policy	A-MSDU Present	Reserved			
QoS Null frames sent by TPU sleep STAs in a nonmesh BSS	TID	Reserved	Ack Policy	Reserved	Reserved			
All frames sent by mesh STAs in a mesh BSS	TID	EOSP	Ack Policy	A-MSDU Present	Mesh Control Present	Mesh Power Save Level	RSPI	Reserved

Source: 802.11 § 8.2.4.5

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	**The wireless network provided by the Ruckus Devices includes a call control level. For example, the Logical Link Control (LLC) Layer is the call control level.**  Figure 11-8—TKIP MIC relation to IEEE 802.11 processing (informative) **Source: 802.11 § 11.4.2.3.2** 

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	**4.2.5 Interaction with other IEEE 802® layers** IEEE Std 802.11 is required to appear to higher layers [logical link control (LLC)] as a wired IEEE 802 LAN. This requires that the IEEE 802.11 network handle STA mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE Std 802.11 to incorporate functionality that is untraditional for MAC sublayers. **Source: 802.11 § 4.2.5**

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	**The wireless network provided by the Ruckus Devices includes a resource control level. For example, the Media Access Control (MAC) Layer is the resource control level.** **4.5.3 Services that support the distribution service** **4.5.3.1 General** The primary purpose of a MAC sublayer is to transfer MSDUs between MAC sublayer entities. The information required for the distribution service to operate is provided by the association services. Before a data message can be handled by the distribution service, a STA is "associated." **Source: 802.11 § 4.5.3.1** 

Claim 1	RUCKUS DEVICES
A method for transferring data with a verified QoS in a communication network, which includes a call control level, a resource control level and at least one terminal assigned to data transfer, comprising:	**The wireless network provided by the Ruckus Devices includes at least one terminal assigned to data transfer. For example, the QoS access point (AP) constitutes a terminal assigned to data transfer.** **access point (AP):** An entity that contains one station (STA) and provides access to the distribution services, via the wireless medium (WM) for associated STAs. **quality-of-service (QoS) facility:** The set of enhanced functions, channel access rules, frame formats, frame exchange sequences and managed objects used to provide parameterized and prioritized QoS. **quality-of-service (QoS) access point (AP):** An AP that supports the QoS facility. The functions of a QoS AP are a superset of the functions of a non-QoS AP, and thus a QoS AP is able to function as a non-QoS AP to non-QoS stations (STAs). **Source: 802.11 § 3.1**

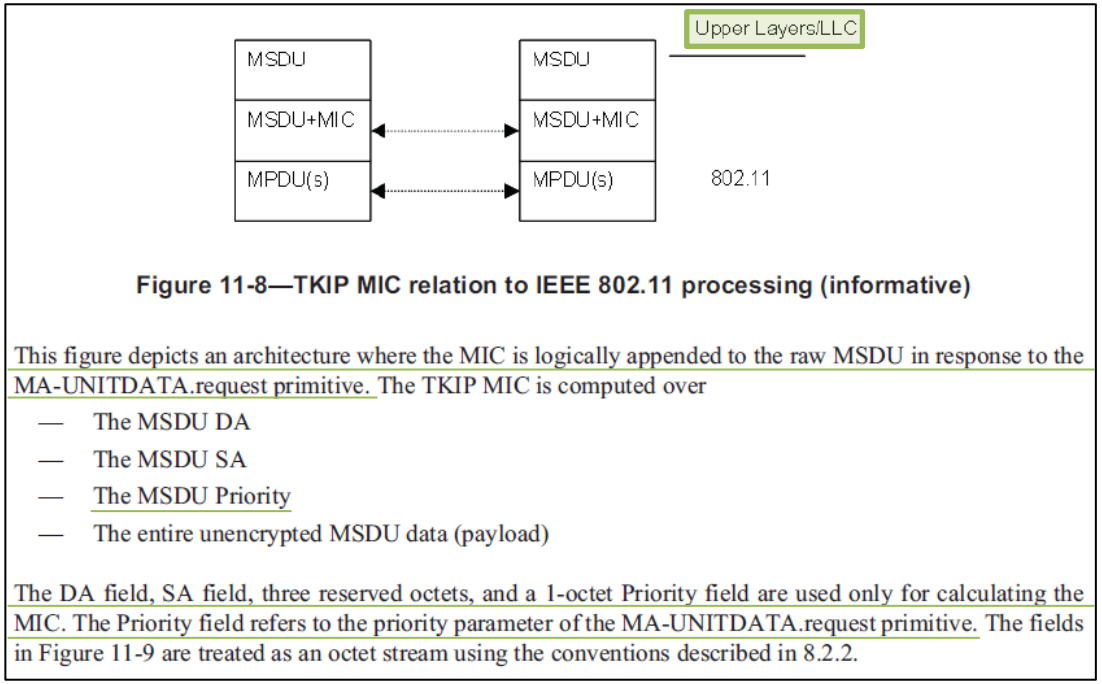
Claim 1	RUCKUS DEVICES
determining a QoS requirement for data transfer and verified at call control level;	**The Ruckus Devices determine a QoS requirement (e.g., the QoS priority parameter) for data transfer (e.g., MSDUs to be delivered). Each MSDU contains a QoS priority parameter.** **5. MAC service definition** **5.1 Overview of MAC services** **5.1.1 Data service** **5.1.1.1 General** This service provides peer LLC entities with the ability to exchange MSDUs. To support this service, the local MAC uses the underlying PHY-level services to transport an MSDU to a peer MAC entity, where it is delivered to the peer LLC. Such asynchronous MSDU transport is performed on a connectionless basis. By default, MSDU transport is on a best-effort basis. However, the QoS facility uses a traffic identifier (TID) to specify differentiated services on a per-MSDU basis. The QoS facility also permits more synchronous behavior to be supported on a connection-oriented basis using TSPECs. There are no guarantees that the submitted MSDU will be delivered successfully. Group addressed transport is part of the data service provided by the MAC. Due to the characteristics of the WM, group addressed MSDUs may experience a lower QoS, compared to that of individually addressed MSDUs. All STAs support the data service, but only QoS STAs in a QoS BSS differentiate their MSDU delivery according to the designated traffic category or traffic stream (TS) of individual MSDUs. Because operation of certain functions of the MAC may cause reordering of some MSDUs, as discussed in more detail below, in non-QoS STAs, there are two service classes within the data service. By selecting the desired service class, each LLC entity initiating the transfer of MSDUs is able to control whether MAC entities are or are not allowed to reorder those MSDUs. There are two service classes available in a QoS STA: QoSAck and QoSNoAck. The service classes are used to signal if the MSDU is to be transmitted with or without using the MAC-level acknowledgment. In QoS STAs either associated in a BSS or having membership in an IBSS, the MAC uses a set of rules that tends to cause higher UP MSDUs in a BSS to be sent before lower UP MSDUs in the BSS. The MAC sublayer entities determine the UPs for MSDUs based on the TID values provided with those MSDUs. If a TSPEC has been provided for a TS, via the MAC sublayer management entity, the MAC attempts to deliver MSDUs belonging to that TS in accordance with the QoS parameter values contained in the TSPEC. In a BSS with some STAs supporting the QoS facility and others not supporting the QoS facility, in delivering an MSDU to a non-QoS STA, the QoS STA uses the access category (AC) corresponding to the UP of the MSDU. **Source: 802.11 § 5.1**

Claim 1	RUCKUS DEVICES
determining a QoS requirement for data transfer and verified at call control level;	**The QoS priority parameter is encoded to the TID which the Ruckus Devices uses to determine a QoS requirement.** **5. MAC service definition** **5.1 Overview of MAC services** **5.1.1 Data service** **5.1.1.1 General** This service provides peer LLC entities with the ability to exchange MSDUs. To support this service, the local MAC uses the underlying PHY-level services to transport an MSDU to a peer MAC entity, where it is delivered to the peer LLC. Such asynchronous MSDU transport is performed on a connectionless basis. By default, MSDU transport is on a best-effort basis. However, the QoS facility uses a traffic identifier (TID) to specify differentiated services on a per-MSDU basis. The QoS facility also permits more synchronous behavior to be supported on a connection-oriented basis using TSPECs. There are no guarantees that the submitted MSDU will be delivered successfully. Group addressed transport is part of the data service provided by the MAC. Due to the characteristics of the WM, group addressed MSDUs may experience a lower QoS, compared to that of individually addressed MSDUs. All STAs support the data service, but only QoS STAs in a QoS BSS differentiate their MSDU delivery according to the designated traffic category or traffic stream (TS) of individual MSDUs. Because operation of certain functions of the MAC may cause reordering of some MSDUs, as discussed in more detail below, in non-QoS STAs, there are two service classes within the data service. By selecting the desired service class, each LLC entity initiating the transfer of MSDUs is able to control whether MAC entities are or are not allowed to reorder those MSDUs. There are two service classes available in a QoS STA: QoSAck and QoSNoAck. The service classes are used to signal if the MSDU is to be transmitted with or without using the MAC-level acknowledgment. In QoS STAs either associated in a BSS or having membership in an IBSS, the MAC uses a set of rules that tends to cause higher UP MSDUs in a BSS to be sent before lower UP MSDUs in the BSS. The MAC sublayer entities determine the UPs for MSDUs based on the TID values provided with those MSDUs. If a TSPEC has been provided for a TS, via the MAC sublayer management entity, the MAC attempts to deliver MSDUs belonging to that TS in accordance with the QoS parameter values contained in the TSPEC. In a BSS with some STAs supporting the QoS facility and others not supporting the QoS facility, in delivering an MSDU to a non-QoS STA, the QoS STA uses the access category (AC) corresponding to the UP of the MSDU. **Source: 802.11 § 5.1**

Claim 1	RUCKUS DEVICES
determining a QoS requirement for data transfer and verified at call control level;	**8.2.4.5.2 TID subfield** The TID subfield identifies the TC or TS to which the corresponding MSDU (or fragment thereof) or A-MSDU in the Frame Body field belongs. The TID subfield also identifies the TC or TS of traffic for which a TXOP is being requested, through the setting of TXOP duration requested or queue size. The encoding of the TID subfield depends on the access policy (see 8.4.2.32) and is shown in Table 8-5. Additional information on the interpretation of the contents of this field appears in 5.1.1.4. **Table 8-5—TID subfield** For QoS Data+CF-Poll, the TID subfield in the QoS Control field indicates the TID of the data. For all QoS (+)CF-Poll frames of subtype Null, the TID subfield in the QoS Control field indicates the TID for which the poll is intended. The requirement to respond to that TID is nonbinding, and a STA may respond with any frame. For STAs where dot11OCBActivated is true, traffic streams are not used and the TID always corresponds to a TC. **Source: 802.11 § 8.2**

Access policy	Usage	Allowed values in bits 0–3 (TID subfield)
EDCA	UP for either TC or TS, regardless of whether admission control is required	0–7
HCCA	TSID	8–15
HEMM	TSID, regardless of the access mechanism used	8–15

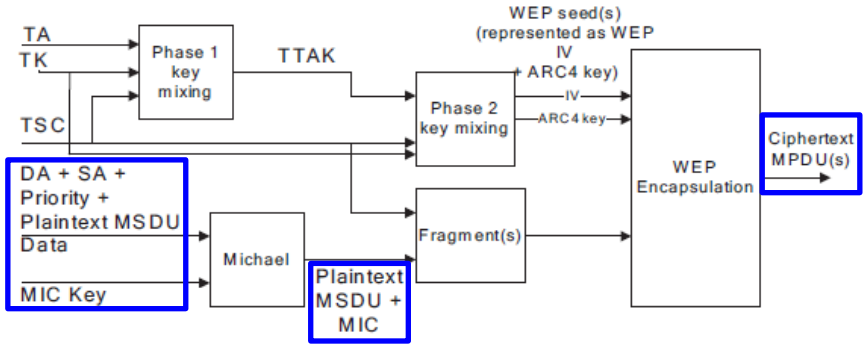
Claim 1	RUCKUS DEVICES
determining a QoS requirement for data transfer and verified at call control level;	**5.1.1.2 Determination of UP** The QoS facility supports eight priority values, referred to as *UPs*. The values a UP may take are the integer values from 0 to 7 and are identical to the IEEE 802.1D priority tags. An MSDU with a particular UP is said to belong to a traffic category (TC) with that UP. The UP is provided with each MSDU at the medium access control service access point (MAC_SAP) either directly, in the UP parameter, or indirectly, in a TSPEC designated by the UP parameter. **5.1.1.3 Determination of UP of received frames at the AP sent by other STAs in the BSS** The received individually addressed frames at the AP may be as follows: a) Non-QoS subtypes, in which case the AP shall assign to them a priority of Contention, if they are received during the contention period (CP), or ContentionFree, if they are received during the contention-free period (CFP). b) QoS subtypes, in which case the AP shall infer the UP value from the TID in the QoS Control field directly for TID values between 0 and 7. For TID values between 8 and 15 the AP shall extract the **Source: 802.11 § 5.1**

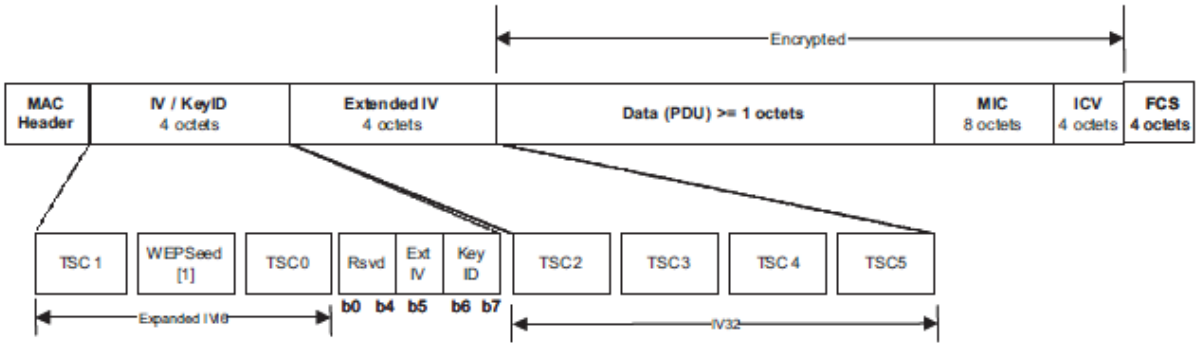
Claim 1	RUCKUS DEVICES
determining a QoS requirement for data transfer and verified at call control level;	**The LLC (call control level) verifies the requirement through the MA-UNITDATA primitive.** **4.3.13.14 QoS traffic capability** QoS traffic capability procedures enable the QoS STA to indicate that it is capable of transmitting traffic belonging to the corresponding user priority (UP) from applications that require generation of such traffic. The QoS Traffic Capability might be used for example as an input to estimate the blocking probability of a voice application based on the number of voice capable non-AP STAs. **Source: 802.11 § 4.3.13.14**  **Figure 11-8—TKIP MIC relation to IEEE 802.11 processing (informative)** This figure depicts an architecture where the MIC is logically appended to the raw MSDU in response to the MA-UNITDATA.request primitive. The TKIP MIC is computed over — The MSDU DA — The MSDU SA — The MSDU Priority — The entire unencrypted MSDU data (payload) The DA field, SA field, three reserved octets, and a 1-octet Priority field are used only for calculating the MIC. The Priority field refers to the priority parameter of the MA-UNITDATA.request primitive. The fields in Figure 11-9 are treated as an octet stream using the conventions described in 8.2.2. **Source: 802.11 § 11.4.2.3.2**

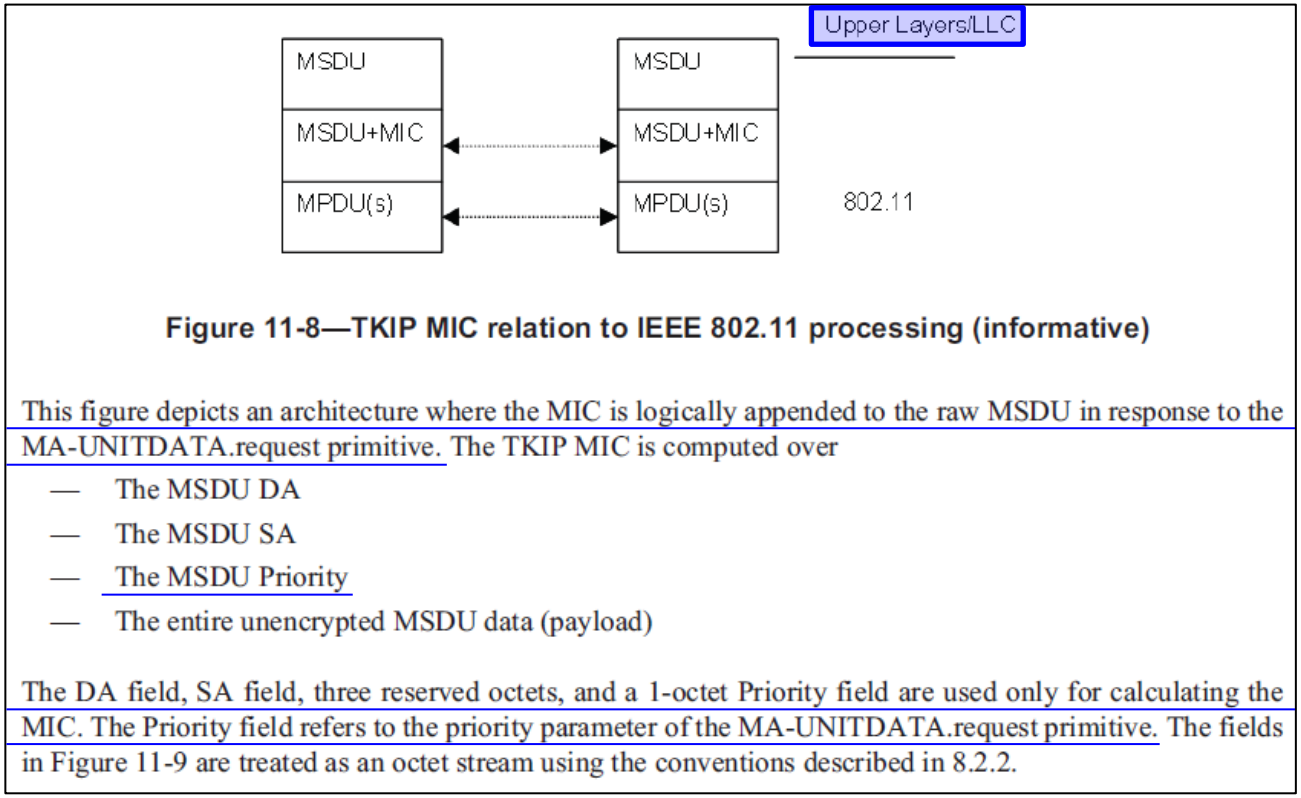
Claim 1	RUCKUS DEVICES
creating and transferring, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal;	**The Ruckus Devices create and transfer, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal. The link layer control generates a service primitive (MA-UNITDATA primitive) that includes priority and service class parameters. Further, the priority parameters in the MPDU header and the MIC value making up the encrypted MPDU is transferred to the MAC sublayer entity. The presence of security encapsulation (e.g., TKIP, CCMP, GCMP and MIC) includes creation of a MIC field (encrypted token).** **cryptographic encapsulation:** The process of generating the cryptographic payload from the plaintext data. This comprises the cipher text as well as any associated cryptographic state required by the receiver of the data, e.g., initialization vectors (IVs), sequence numbers, message integrity codes (MICs), key identifiers. **message integrity code (MIC):** A value generated by a cryptographic function. If the input data are changed, a new value cannot be correctly computed without knowledge of the cryptographic key(s) used by the cryptographic function. NOTE—This is traditionally called a *message authentication code* (MAC), but the acronym MAC is already reserved for another meaning in this standard. **Source: 802.11 § 3.1**

Claim 1	RUCKUS DEVICES
creating and transferring, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal;	**4.5.4.4 Data confidentiality** In a wired LAN, only those STAs physically connected to the wire can send or receive LAN traffic. With a wireless shared medium, there is no physical connection, and all STAs and certain other RF devices in or near the LAN might be able to send, receive, and/or interfere with the LAN traffic. An IEEE 802.11-compliant STA can receive like-PHY IEEE 802.11 traffic that is within range and can transmit to any other IEEE 802.11 STA within range. Thus, the connection of a single wireless link (without data confidentiality) to an existing wired LAN may seriously degrade the security level of the wired LAN. To bring the security of the WLAN up to the level implicit in wired LAN design, IEEE Std 802.11 provides the ability to protect the contents of messages. This functionality is provided by the data confidentiality service. Data confidentiality is an SS. IEEE Std 802.11 provides several cryptographic algorithms to protect data traffic, including: WEP, TKIP, and CCMP. WEP and TKIP are based on the ARC4[19] algorithm, and CCMP is based on the advanced encryption standard (AES). A means is provided for STAs to select the algorithm(s) to be used for a given association. IEEE Std 802.11 provides one security protocol, CCMP, for protection of individually addressed robust management frames. This standard does not provide data confidentiality for group addressed robust management frames. IEEE Std 802.11 provides one security protocol, CCMP, for protection of individually addressed and group addressed data frames between mesh STAs. **Source: 802.11 § 4.5.4**

Claim 1	RUCKUS DEVICES
creating and transferring, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal;	**5.1.2 Security services** Security services in IEEE Std 802.11 are provided by the authentication service and the CCMP and BIP mechanisms. The scope of the security services provided is limited to station-to-station data and robust management frame transmissions. When CCMP is used, the data confidentiality service is provided for data frames and individually addressed robust management frames. For the purposes of this standard, CCMP is viewed as a logical service located within the MAC sublayer as shown in the reference model, Figure 4-14 (in 4.9). Actual implementations of CCMP are transparent to the LLC and other layers above the MAC sublayer. **Source: 802.11 § 5.1.2**

Claim 1	RUCKUS DEVICES
creating and transferring, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal;	**11.4.2.1.2 TKIP cryptographic encapsulation** TKIP enhances the WEP cryptographic encapsulation with several additional functions, as depicted in Figure 11-5.  **Figure 11-5—TKIP encapsulation block diagram** a) TKIP MIC computation protects the MSDU Data field and corresponding SA, DA, and Priority fields. The computation of the MIC is performed on the ordered concatenation of the SA, DA, Priority, and MSDU Data fields. The MIC is appended to the MSDU Data field. TKIP discards any MIC padding prior to appending the MIC. b) If needed, IEEE Std 802.11 fragments the MSDU with MIC into one or more MPDUs. TKIP assigns a monotonically increasing TSC value to each MPDU, taking care that all the MPDUs generated from the same MSDU have the same value of extended IV (see 11.4.2.2). c) For each MPDU, TKIP uses the key mixing function to compute the WEP seed. d) TKIP represents the WEP seed as a WEP IV and ARC4 key and passes these with each MPDU to WEP for generation of the ICV (see 8.2.4.7), and for encryption of the plaintext MPDU, including all or part of the MIC, if present. WEP uses the WEP seed as a WEP default key, identified by a key identifier associated with the temporal key. NOTE—When the TSC space is exhausted, the choices available to an implementation are to replace the temporal key with a new one or to end communications. Reuse of any TSC value compromises already sent traffic. Note that retransmitted MPDUs reuse the TSC without any compromise of security. The TSC is large enough, however, that TSC space exhaustion is not expected to be an issue. In Figure 11-5, the TKIP-mixed transmit address and key (TTAK) denotes the intermediate key produced by Phase 1 of the TKIP mixing function (see 11.4.2.5). **Source: 802.11 § 11.4.2.1**

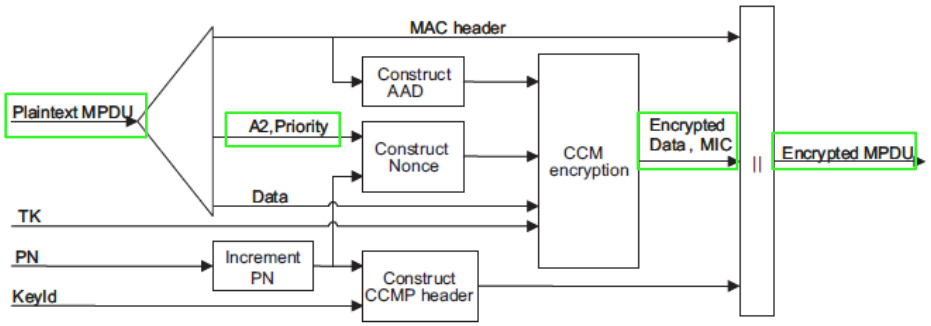
Claim 1	RUCKUS DEVICES
creating and transferring, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal;	**11.4.2.2 TKIP MPDU formats** TKIP reuses the pre-RSNA WEP MPDU format. It extends the MPDU by 4 octets to accommodate an extension to the WEP IV, denoted by the Extended IV field, and extends the MSDU format by 8 octets to accommodate the new MIC field. TKIP inserts the Extended IV field immediately after the WEP IV field and before the encrypted data. TKIP appends the MIC to the MSDU Data field; the MIC becomes part of the encrypted data. Once the MIC is appended to the MSDU data, the added MIC octets are considered part of the MSDU for subsequent fragmentation. Figure 11-7 depicts the layout of the encrypted MPDU when using TKIP. Note that the figure only depicts the case when the MSDU can be encapsulated in a single MPDU.  **Figure 11-7—Construction of expanded TKIP MPDU** **Source: 802.11 § 11.4.2.2**

Claim 1	RUCKUS DEVICES
creating and transferring, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal;	 **Figure 11-8—TKIP MIC relation to IEEE 802.11 processing (informative)** This figure depicts an architecture where the MIC is logically appended to the raw MSDU in response to the MA-UNITDATA.request primitive. The TKIP MIC is computed over — The MSDU DA — The MSDU SA — The MSDU Priority — The entire unencrypted MSDU data (payload) The DA field, SA field, three reserved octets, and a 1-octet Priority field are used only for calculating the MIC. The Priority field refers to the priority parameter of the MA-UNITDATA.request primitive. The fields in Figure 11-9 are treated as an octet stream using the conventions described in 8.2.2. **Source: 802.11 § 11.4.2.3**

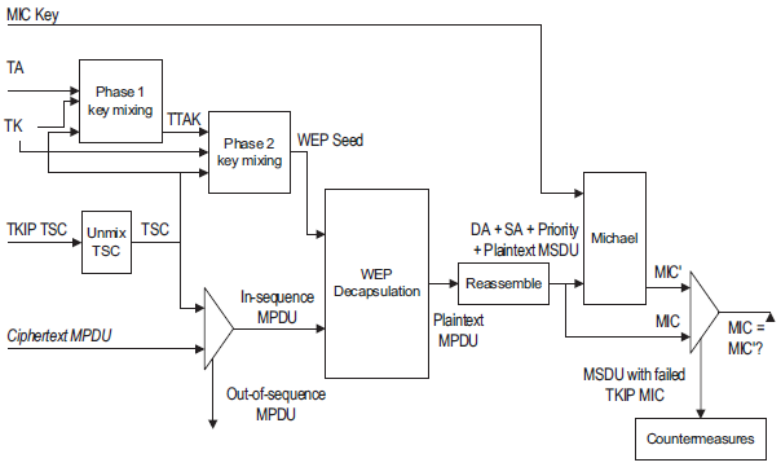
Claim 1	RUCKUS DEVICES
creating and transferring, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal;	**5.2.2.4 Effect of receipt** On receipt of this primitive, the MAC sublayer entity determines whether it is able to fulfill the request according to the requested parameters. A request that cannot be fulfilled according to the requested parameters is discarded, and this action is indicated to the LLC sublayer entity using an MA-UNITDATA-STATUS.indication primitive that describes why the MAC was unable to fulfill the request. If the request can be fulfilled according to the requested parameters, the MAC sublayer entity appends all MAC specified fields (including DA, SA, FCS, and all fields that are unique to IEEE Std 802.11), passes the properly formatted frame to the lower layers for transfer to a peer MAC sublayer entity or entities (see 5.1.4), and indicates this action to the LLC sublayer entity using an MA-UNITDATA-STATUS.indication primitive with transmission status set to Successful. **Source: 802.11 § 5.2.2.4**

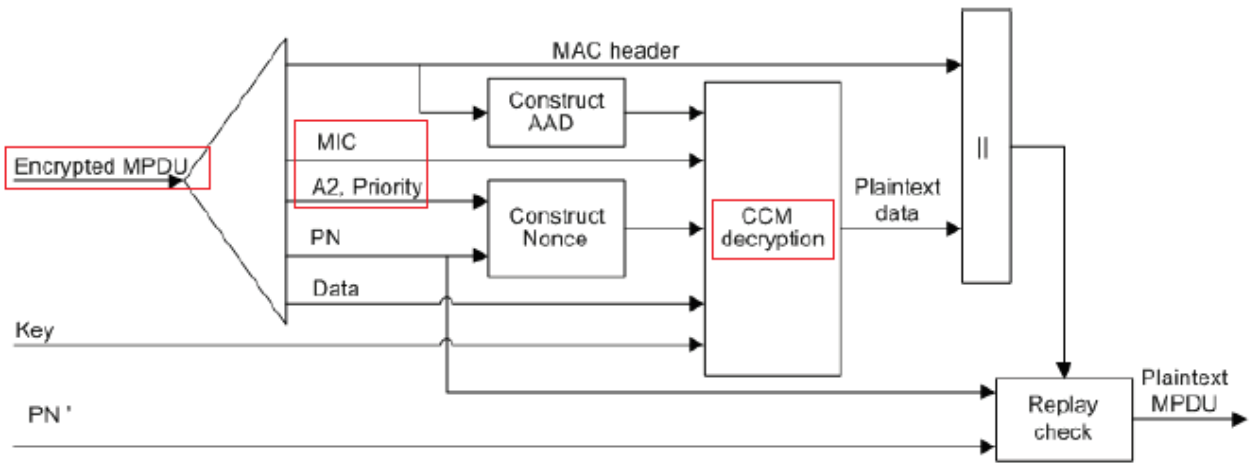
Claim 1	RUCKUS DEVICES
creating and transferring, taking into account the QoS requirement verified at the call control level, at least one encrypted token to the terminal;	**The priority parameter specifies requested priority of the data unit transfer and the service class parameter specifies the requested service class of the data unit transfer.** **5.2.2.2 Semantics of the service primitive** The parameters of the primitive are as follows: MA-UNITDATA.request(source address, destination address, routing information, data, priority, service class) The source address (SA) parameter specifies an individual MAC sublayer address of the sublayer entity from which the MSDU is being transferred. The destination address (DA) parameter specifies either an individual or a group MAC sublayer entity address. The routing information parameter specifies the route desired for the data transfer (a null value indicates source routing is not to be used). For IEEE Std 802.11, the routing information parameter shall be null. The data parameter specifies the MSDU to be transmitted by the MAC sublayer entity. For IEEE Std 802.11, the length of the MSDU shall be less than or equal to 2304 octets. The priority parameter specifies the priority desired for the data unit transfer. The allowed values of priority are described in 5.1.1.4. The service class parameter specifies the service class desired for the data unit transfer. The allowed values of service class are described in 5.1.1.5 and 5.1.3. **Source: 802.11 § 5.2.2.2**

Claim 1	RUCKUS DEVICES
transferring the verified QoS requirement and the encrypted token to the resource control level from the terminal;	**The Ruckus Devices transfer the verified QoS requirement and the encrypted token to the resource control level from the terminal. The priority parameters in the MPDU header and the MIC value making up the encrypted MPDU are transferred to the MAC sublayer entity.** **11.4 RSNA confidentiality and integrity protocols** **11.4.1 Overview** This standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP. This standard defines one integrity protocol for management frames: BIP. Implementation of TKIP is optional for an RSNA and used only for the protection of data frames. A design aim for TKIP was that the algorithm should be implementable within the capabilities of most devices supporting only WEP, so that many such devices would be field-upgradable by the supplier to support TKIP. BIP is a mechanism that is used only when management frame protection is negotiated. BIP provides integrity protection for group addressed robust management frames. BIP is only used to protect management frames within the BSS. **11.4.2 Temporal Key Integrity Protocol (TKIP)** **11.4.2.1 TKIP overview** **11.4.2.1.1 General** The TKIP is a cipher suite enhancing WEP on pre-RSNA hardware. TKIP modifies WEP as follows: a) A transmitter calculates a keyed cryptographic message integrity code (MIC) over the MSDU SA and DA, the MSDU priority (see 11.4.2.3), and the MSDU plaintext data. TKIP appends the computed MIC to the MSDU data prior to fragmentation into MPDUs. The receiver verifies the MIC after decryption, ICV checking, and defragmentation of the MPDUs into an MSDU and discards any received MSDUs with invalid MICs. TKIP's MIC provides a defense against forgery attacks. **Source: 802.11 § 11.4**

Claim 1	RUCKUS DEVICES
transferring the verified QoS requirement and the encrypted token to the resource control level from the terminal;	The CCMP cryptographic encapsulation process is depicted in Figure 11-17.  **Figure 11-17—CCMP encapsulation block diagram** CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following steps: a) Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key. Note that retransmitted MPDUs are not modified on retransmission. b) Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being masked to 0 when calculating the AAD. c) Construct the CCM Nonce block from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2. d) Place the new PN and the key identifier into the 8-octet CCMP header. e) Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and MIC. This step is known as CCM originator processing. f) Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and MIC, as described in 11.4.3.2. The CCM reference describes the processing of the key, nonce, AAD, and data to produce the encrypted output. See 11.4.3.3.2 to 11.4.3.3.6 for details of the creation of the AAD and nonce from the MPDU and the associated MPDU-specific processing. **Source: 802.11 § 11.4**

Claim 1	RUCKUS DEVICES
decrypting, at the resource control level, the encrypted token, and verifying the QoS requirement using the decrypted token; and	**The Ruckus Devices decrypt, at the resource control level (e.g., MLME/SME), the encrypted token, and verify the QoS requirement using the decrypted token. The sublayer (e.g., the MLME or SME) decrypts encrypted frame body including the MIC. The priority parameter specifies requested priority of the data unit transfer and the service class parameter specifies the requested service class of the data unit transfer. Further the MAC sublayer which acts as the resource control level, determines whether it is able to fulfil the request based on the priority requested.** If dot11MgmtOptionQoSTrafficCapabilityActivated is true, a non-AP QoS shall construct the QoS Traffic Capability Flags as specified in 8.4.2.80 and 8.5.14.22. QoS Traffic Capability Flags are constructed at the SME of the non-AP QoS STA, from application requirements supplied to the SME. The QoS Traffic Capability Flags are constructed from two application requirements: whether generation of traffic is required for applications and whether a specific UP is required for the generated traffic. If such requirements are supplied to the SME, the SME shall set the flag corresponding to the specific UP to 1. NOTE—The requirements might be known before the traffic is actually generated. For example, a phone application might configured to generate UP 6 traffic upon the initiation of a voice session. Unless application requirements for a specific UP are supplied to the SME, the SME shall set the flag corresponding to the UP to 0. If dot11MgmtOptionQoSTrafficCapabilityActivated is true, a non-AP QoS STA shall include the QoS Traffic Capability element in an Association Request frame or in a Reassociation Request frame when it is sending such a frame to associate or reassociate with an AP. If there is any change in QoS Traffic Capability Flags while associated with an AP, the non-AP STA shall send a QoS Traffic Capability Update frame (see 8.5.14.22) including the updated QoS Traffic Capability Flags to the AP. **Source: 802.11 § 10.23**

Claim 1	RUCKUS DEVICES
decrypting, at the resource control level, the encrypted token, and verifying the QoS requirement using the decrypted token; and	**11.4.2.1.3 TKIP decapsulation** TKIP enhances the WEP decapsulation process with the following additional steps: a) Before WEP decapsulates a received MPDU, TKIP extracts the TSC sequence number and key identifier from the WEP IV and the extended IV. TKIP discards a received MPDU that violates the sequencing rules (see 11.4.2.6) and otherwise uses the mixing function to construct the WEP seed. b) TKIP represents the WEP seed as a WEP IV and ARC4 key and passes these with the MPDU to WEP for decapsulation. c) If WEP indicates the ICV check succeeded, the implementation reassembles the MPDU into an MSDU. If the MSDU defragmentation succeeds, the receiver verifies the TKIP MIC. If MSDU defragmentation fails, then the MSDU is discarded. d) The MIC verification step recomputes the MIC over the MSDU SA, DA, Priority, and MSDU Data fields (but not the TKIP MIC field). The calculated TKIP MIC result is then compared bit-wise to the received MIC. e) If the received and the locally computed MIC values are identical, the verification succeeds, and TKIP shall deliver the MSDU to the upper layer. If the two differ, then the verification fails; the receiver shall discard the MSDU and shall engage in appropriate countermeasures. Figure 11-6 depicts this process.  **Figure 11-6—TKIP decapsulation block diagram** **Source: 802.11 § 10.23**

Claim 1	RUCKUS DEVICES
decrypting, at the resource control level, the encrypted token, and verifying the QoS requirement using the decrypted token; and	Figure 11-21 depicts the CCMP decapsulation process.  **Figure 11-21—CCMP decapsulation block diagram** CCMP decrypts the payload of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps: a) The encrypted MPDU is parsed to construct the AAD and nonce values. b) The AAD is formed from the MPDU header of the encrypted MPDU. c) The Nonce value is constructed from the A2, PN, and Nonce Flags fields. d) The MIC is extracted for use in the CCM integrity checking. e) The CCM recipient processing uses the temporal key, AAD, nonce, MIC, and MPDU cipher text data to recover the MPDU plaintext data as well as to check the integrity of the AAD and MPDU plaintext data. **Source: 802.11 § 11.4**

Claim 1	RUCKUS DEVICES
configuring the communication network taking into account the QoS requirement verified, such that the data is transferred with the verified QoS.	**The Ruckus Devices configure the communication network taking into account the QoS requirement verified, such that the data is transferred with the verified QoS. The original MPDU header is concatenated with the plaintext MPDU and is processed according to QoS parameters in HCF contention based channel access (EDCA).** **enhanced distributed channel access (EDCA):** The prioritized carrier sense multiple access with collision avoidance (CSMA/CA) access mechanism used by quality-of-service (QoS) stations (STAs) in a QoS basic service set (BSS). This access mechanism is also used by the QoS access point (AP) and operates concurrently with hybrid coordination function (HCF) controlled channel access (HCCA). **hybrid coordination function (HCF):** A coordination function that combines and enhances aspects of the contention-based and contention-free access methods to provide quality-of-service (QoS) stations (STAs) with prioritized and parameterized QoS access to the wireless medium (WM), while continuing to support non-QoS STAs for best-effort transfer. The HCF includes the functionality provided by both enhanced distributed channel access (EDCA) and HCF controlled channel access (HCCA). The HCF is compatible with the distributed coordination function (DCF) and the point coordination function (PCF). It supports a uniform set of frame formats and exchange sequences that STAs might use during both the contention period (CP) and the contention-free period (CFP). **hybrid coordinator (HC):** A type of coordinator, defined as part of the quality-of-service (QoS) facility, that implements the frame exchange sequences and medium access control (MAC) service data unit (MSDU) handling rules defined by the hybrid coordination function (HCF). The HC operates during both the contention period (CP) and contention-free period (CFP). The HC performs bandwidth management including the allocation of transmission opportunities (TXOPs) to QoS stations (STAs). The HC is collocated with a QoS access point (AP). **hybrid coordination function (HCF) controlled channel access (HCCA):** The channel access mechanism utilized by the hybrid coordinator (HC) to coordinate contention-free media use by quality-of-service (QoS) stations (STAs) for downlink individually addressed, uplink, and direct-link transmissions. **Source: 802.11 § 3.1**

Claim 1	RUCKUS DEVICES
configuring the communication network taking into account the QoS requirement verified, such that the data is transferred with the verified QoS.	**9.2.4 Hybrid coordination function (HCF)** **9.2.4.1 General** The QoS facility includes an additional coordination function called *HCF* that is only usable in QoS network configurations. The HCF shall be implemented in all QoS STAs except mesh STAs. Instead, mesh STAs implement the MCF. The HCF combines functions from the DCF and PCF with some enhanced, QoS-specific mechanisms and frame subtypes to allow a uniform set of frame exchange sequences to be used for QoS data transfers during both the CP and CFP. The HCF uses both a contention-based channel access method, called the *enhanced distributed channel access* (EDCA) mechanism for contention-based transfer and a controlled channel access, referred to as the *HCF controlled channel access* (HCCA) mechanism, for contention-free transfer. STAs may obtain TXOPs using one or both of the channel access mechanisms specified in 9.19. If a TXOP is obtained using the contention-based channel access, it is defined as *EDCA TXOP*. If a TXOP is obtained using the controlled channel access, it is defined as *HCCA TXOP*. If an HCCA TXOP is obtained due to a QoS (+)CF-Poll frame from the HC, the TXOP is defined as a *polled TXOP*. Time priority management frames are transmitted outside of the normal MAC queuing process as per individually described transmission rules. Frames listed in Table 8-229 with a value of "Yes" in the "Time Priority" column are time priority management frames. No other frames are time priority management frames. **Source: 802.11 § 9.2.4**

Claim 1	RUCKUS DEVICES
configuring the communication network taking into account the QoS requirement verified, such that the data is transferred with the verified QoS.	**9.2.4.2 HCF contention-based channel access (EDCA)** The EDCA mechanism provides differentiated, distributed access to the WM for STAs using eight different UPs. The EDCA mechanism defines four access categories (ACs) that provide support for the delivery of traffic with UPs at the STAs. The AC is derived from the UPs as shown in Table 9-1. **Table 9-1—UP-to-AC mappings** Priority: Lowest → Highest | UP (Same as 802.1D user priority) | 802.1D designation | AC | Designation (informative) | |---|---|---|---| | 1 | BK | AC_BK | Background | | 2 | — | AC_BK | Background | | 0 | BE | AC_BE | Best Effort | | 3 | EE | AC_BE | Best Effort | | 4 | CL | AC_VI | Video | | 5 | VI | AC_VI | Video | | 6 | VO | AC_VO | Voice | | 7 | NC | AC_VO | Voice | **Source: 802.11 § 9.2.4**

Claim 1	RUCKUS DEVICES
configuring the communication network taking into account the QoS requirement verified, such that the data is transferred with the verified QoS.	**9.2.4.2 HCF contention-based channel access (EDCA)** The EDCA mechanism provides differentiated, distributed access to the WM for STAs using eight different UPs. The EDCA mechanism defines four access categories (ACs) that provide support for the delivery of traffic with UPs at the STAs. The AC is derived from the UPs as shown in Table 9-1. **Table 9-1—UP-to-AC mappings** Priority: Lowest → Highest | UP (Same as 802.1D user priority) | 802.1D designation | AC | Designation (informative) | |---|---|---|---| | 1 | BK | AC_BK | Background | | 2 | — | AC_BK | Background | | 0 | BE | AC_BE | Best Effort | | 3 | EE | AC_BE | Best Effort | | 4 | CL | AC_VI | Video | | 5 | VI | AC_VI | Video | | 6 | VO | AC_VO | Voice | | 7 | NC | AC_VO | Voice | **Source: 802.11 § 9.2.4**

Claim 1	RUCKUS DEVICES
configuring the communication network taking into account the QoS requirement verified, such that the data is transferred with the verified QoS.	The QoS AP shall announce the EDCA parameters in selected Beacon frames and in all Probe Response and (Re)Association Response frames by the inclusion of the EDCA Parameter Set element using the information from the MIB entries in dot11EDCATable. If no such element is received, the STAs shall use the default values for the parameters. The fields following the QoS Info field in the EDCA Parameter Set element shall be included in all Beacon frames occurring within two (optionally more) delivery traffic indication map (DTIM) periods following a change in AC parameters, which provides all STAs an opportunity to receive the updated EDCA parameters. A QoS STA shall update its MIB values of the EDCA parameters within an interval of time equal to one beacon interval after receiving an updated EDCA parameter set. QoS STAs update the MIB attributes and store the EDCA Parameter Set update count value in the QoS Info field. An AP may change the EDCA access parameters by changing the EDCA Parameter Set element in the Beacon frame, Probe Response frame, and (Re)Association Response frame. However, the AP should change them only rarely. A QoS STA shall use the EDCA Parameter Set Update Count Value subfield in the QoS Capability element of all Beacon frames to determine whether the STA is using the current EDCA Parameter Values. If the EDCA Parameter Set update count value in the QoS Capability element is different from the value that has been stored, the QoS STA shall query the updated EDCA parameter values by sending a Probe Request frame to the AP. **Source: 802.11 § 9.2.4**